На правах рукописи

Зубова Марина Александровна

Компьютерная информация как объект уголовно-правовой охраны

Специальность: 12.00.08 – уголовное право и криминология;
уголовно-исполнительное право

Автореферат
диссертации на соискание ученой степени
кандидата юридических наук

Казань – 2008

Работа выполнена на кафедре уголовного права государственного образовательного учреждения высшего профессионального образования «Казанский государственный университет им. В.И. Ульянова-Ленина».

Научный руководитель: доктор юридических наук, профессор
Талан Мария Вячеславовна
(Казанский государственный университет им. В.И. Ульянова-Ленина)

Официальные оппоненты: доктор юридических наук, профессор
Чучаев Александр Иванович
(Московская государственная юридическая академия);
кандидат юридических наук, доцент
Селивановская Юлия Игоревна
(Казанский государственный технический университет им. А.Н. Туполева)

Ведущая организация: **Казанский филиал Российской академии правосудия**

Защита состоится «30» октября 2008г. в 12 часов на заседании объединенного совета по защите докторских и кандидатских диссертаций ДМ 212.081.12 при Казанском государственном университете им. В.И. Ульянова-Ленина по адресу: 420008, г. Казань, ул. Кремлевская, д. 18, ауд. 335.

С диссертацией можно ознакомиться в научной библиотеке государственного образовательного учреждения высшего профессиональ-ного образования «Казанский государственный университет им. В.И. Ульянова-Ленина».

Автореферат разослан «___» сентября 2008г.

Ученый секретарь
диссертационного совета,
кандидат юридических наук, доцент А.Р. Каюмова

Актуальность темы диссертационного исследования. В связи с социально-экономическими изменениями, произошедшими в России в конце XX в., переходом к информационному обществу, появился новый вид общественных отношений – отношения в области обращения информации. Информация стала одним из необходимых элементов жизни общества. Разные ее виды проникли практически во все сферы общественной жизни. Право не осталось в стороне от произошедших изменений: начала развиваться новая комплексная отрасль права – информационное право. По мере формирования и развития информационного права как самостоятельной отрасли российского права будет развиваться в самостоятельную отрасль юридической науки наука информационного права. Это нашло отражение в Основном законе РФ, который в качестве неотъемлемого компонента правового статуса личности рассматривает право на информационную безопасность. С появлением и развитием компьютерной техники появился еще один вид информации – компьютерная. В силу экономических факторов, отставания России в техническом развитии от зарубежных стран, сначала отношения в сфере обращения компьютерной информации развивались медленно. Но с совершенствованием экономики, научно-технического прогресса они также получили дальнейший импульс. Возникновение нового вида отношений неизбежно приводит к тому, что рано или поздно появляется необходимость в их охране. Так, в 1992 году были приняты Законы Российской Федерации «О правовой охране программ для электронно-вычислительных машин и баз данных», «О правовой охране топологий для интегральных микросхем». Большую роль в развитии данного направления сыграл Закон Российской Федерации «О государственной тайне». Но самым важным шагом, предпринятым законодателем, является включение в Уголовный кодекс Российской Федерации новой главы 28

«Преступления в сфере компьютерной информации», содержащей 3 статьи. Первоначальный проект Кодекса содержал 5 статей, но в дальнейшей редакции три первые статьи были объединены в одну.

На XI Конгрессе ООН по предупреждению преступности и уголовному правосудию, прошедшем в апреле 2005 года, преступности, связанной с использованием компьютеров, было уделено особое внимание. В рекомендациях, подготовленных к Конгрессу, эксперты ООН говорят об особом характере киберпреступности и необходимости применения комплексных подходов в борьбе с ней, а также о неотложных мерах по обновлению уголовного законодательства государств-участников ООН, таких как уточнение или изъятие норм, не отвечающих сложившейся ситуации, или принятие норм, касающихся новых видов киберпреступлений[1]. Результатом деятельности Конгресса стала Бангкокская декларация, в которой отмечается, что в период глобализации быстрое развитие информационных технологий и новых систем телекоммуникаций и компьютерных сетей сопровождается злоупотреблениями этими технологиями в преступных целях, а также подчеркивается необходимость разработки национальных мер и развития международного сотрудничества по противодействию киберпреступности. В Концепции национальной безопасности Российской Федерации отмечается, что усиливаются угрозы национальной безопасности Российской Федерации в информационной сфере. Серьезными проблемами являются нарушение нормального функционирования информационных и телекоммуникационных систем, обеспечение сохранности информационных ресурсов, получение несанкционированного доступа к ним[2].

---

[1] Семинар-практикум 6: Меры по борьбе против преступлений, связанных с использованием компьютеров //Материалы Одиннадцатого Конгресса Организации Объединенных Наций по предупреждению преступности и уголовному правосудию.A/CONF.203/14.-Бангкок, 2005.- С.25.

[2] http://www.nationalsecurity.ru/library/00002/

Как отметил в Послании Федеральному Собранию Российской Федерации Президент В.В. Путин, национальные проекты РФ получили инновационную направленность, а это означает, что «государственную поддержку получают именно те направления развития, которые связаны с использованием и внедрением самых передовых технологий. Здесь и компьютеризация всех школ, и обеспечение доступа к Интернету»[3]. Быстрота развития информационных технологий требует динамичности законодательства. Уголовное законодательство должно отражать изменения видов преступлений в сфере компьютерной информации, способов их совершения, а также современное состояние развития информационных технологий и соответствующего отраслевого законодательства.

С момента принятия УК РФ прошло уже больше 10 лет, и можно подвести некоторые итоги. Так, количество зарегистрированных преступлений в сфере компьютерной информации в январе 2008 г. составило 803, в феврале – 1622, в марте – 2984, в апреле – 3510, в мае – 4293, в июне – 5502, а в июле уже 5899[4]. Таким образом, наблюдается их значительный рост. Наибольшую общественную опасность в настоящее время представляют преступления, предусмотренные ст. 272, т.е. неправомерный доступ к компьютерной информации. Однако норма, предусмотренная ст. 274 (нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети), не находит применения на практике. За это время произошли как социально-экономические, так и научно-технические перемены. Как в теории, так и в практике применения ст. 272-274 УК РФ выявились значительные противоречия. Среди основных их причин можно выделить следующие: не совсем удачные конструкции норм о

[3] http://president.kremlin.ru/appears/2007/04/26/1156_type63372type63374type82634_125339.shtml
[4] http://www.mvd.ru/stats/

преступлениях в сфере компьютерной информации, неверное их толкование, не соответствующее действительности представление о значении указанных норм в охране общественных отношений. Особую актуальность тема приобретает в условиях вступления в силу с 1 января 2008 года IV части Гражданского кодекса. Зарубежное законодательство в этом направлении развивается значительно быстрее отечественного. Существуют также и международно-правовые нормы, такие как Конвенция о киберпреступности 2001 г., не ратифицированная Российской Федерацией. Поэтому актуален анализ соответствия действующих норм об ответственности за преступления в сфере компьютерной информации современному законодательству и практике. Преступления в сфере компьютерной информации характеризуются наивысшей степенью латентности (порядка 85-90%), при этом ущерб, наносимый ими, порой является весьма значительным. С учетом всех этих обстоятельств необходимо пересмотреть действующее уголовное законодательство о преступлениях в сфере компьютерной информации и практику его применения. Указанными причинами и обусловлен выбор темы данного диссертационного исследования.

Цели и задачи диссертационного исследования. Целью данного исследования является изучение и анализ норм уголовного закона РФ об ответственности за преступления в сфере компьютерной информации, опыта применения существующего уголовного законодательства и разработка конкретных предложений по его изменению и дополнению в условиях вступления в силу IV части Гражданского кодекса РФ, посвященной интеллектуальной собственности.

Достижение этих целей обеспечивается решением **задач**:

- определения круга информационных отношений, а также сферы их уголовно-правового регулирования;

- анализа международно-правовых норм и норм зарубежного законодательства о преступлениях в сфере компьютерной информации;
- характеристики признаков составов преступлений в сфере компьютерной информации;
- рассмотрения вопросов назначения наказания за преступления в сфере компьютерной информации по уголовному праву России;
- разработки конкретных рекомендаций по совершенствованию законодательства о преступлениях в сфере компьютерной информации и практики его применения.

Объект исследования. Объектом диссертационного исследования являются проблемы уголовно-правовой охраны компьютерной информации.

Предметом исследования выступают:

- правовые нормы о преступлениях в сфере компьютерной информации, содержащиеся в отечественном и зарубежном законодательстве;
- нормы других отраслей права, регулирующие информационные отношения;
- научные публикации, диссертационные исследования;
- материалы следственной и судебной практики.

Методологическая основа исследования. Методологическую основу исследования составляет совокупность общенаучных и частно-научных методов. В числе общенаучных методов были использованы: диалектический метод, метод анализа и синтеза составных частей,

логический метод. Применялись также и специальные методы (сравнительного правоведения, исторический, социологический).

Теоретической основой диссертационного исследования стали труды ученых в области уголовного права, криминологии, теории права и информатики. Тенденции современной преступности и пути уголовно-правового противодействия ей рассматриваются в научных трудах Л.Л. Кругликова, В. В. Лунеева, Э. Ф. Побегайло, А. Я. Сухарева, А.И. Чучаева и др. Правовым проблемам информатизации российского общества и защиты информации посвящены работы Ю. М. Батурина, И. Л. Бачило, В. М. Боера, В. Б. Вехова, А. Г. Волеводза, О. А. Городова, В. А. Копылова, В. В. Крылова, В. Д. Курушина, В. Н. Лопатина, Ю. И. Ляпунова, В. А. Мазурова, В. А. Мещерякова и др.

Уголовно-правовые и криминологические аспекты противодействия преступлениям в сфере компьютерной информации получили дальнейшее развитие в диссертационных исследованиях С. Д. Бражника, Л.А. Букалеровой, С. Ю. Бытко, В. В. Воробьева, М. Ю. Дворецкого, У. В. Зининой, Д. А. Зыкова, А. Ж. Кабановой, В. С. Карпова, Т. П. Кесареевой, А. П. Кузнецова, Д. Г. Малышенко, Т. Г. Смирновой, С. И. Ушакова, А. Е. Шаркова и др. Отдельные вопросы материального права, характеристики личности преступника, профилактики компьютерных преступлений рас-сматриваются в диссертациях С. А. Васютина, Ю. В. Гаврилина, М. В. Евдокимова, А. С. Егорышева, А. В. Касаткина, С. В. Крыгина и др.

Нормативную основу диссертационного исследования составили Конституция России 1993 года, Уголовный кодекс РФ 1996 года (в действующей редакции), IV часть Гражданского кодекса РФ, гражданское законодательство РФ, регулирующее отношения в сфере защиты информации (в частности, Законы «Об авторском праве и смежных правах»,

«О государственной тайне», «Об информации, информационных технологиях и о защите информации», «Об участии в международном информационном обмене»).

Изучены международно-правовые акты, имеющие отношение к теме исследования.

Проанализированы соответствующие подзаконные нормативные источники РФ, уголовное законодательство ряда зарубежных государств (Великобритании, Германии, Испании, Польши, США, Франции, Швейцарии, Швеции и др.).

Эмпирическую основу диссертации составили: материалы следственной и судебной практики по РФ за 1999–2006 гг., статистические данные, полученные отделом «Р» УВД Ульяновской области за 2004–2006 гг., результаты изучения 25 уголовных дел о преступлениях в сфере компьютерной информации в г. Ульяновске, данные социологического исследования 200 пользователей ЭВМ в г. Ульяновске.

Научная новизна диссертации состоит в том, что она представляет собой одно из специальных монографических исследований института уголовной ответственности за преступления в сфере компьютерной информации по российскому уголовному законодательству в условиях вступления в силу IV части Гражданского кодекса РФ, регулирующей отношения в области интеллектуальной собственности.

Основные положения, выносимые на защиту:

1. Необходимо дать определение понятия «компьютерная информация» и вынести его в примечание к статье 272 УК РФ. Компьютерной информацией являются положения объективной действительности, способные изменять характер общественных отношений, являющиеся результатом человеческой деятельности и закрепленные на машинном

носителе, электронно-вычислительной машине, системе ЭВМ, их сети, то есть информация, представленная в электронном виде.

2. Преступлениями в сфере компьютерной информации следует считать виновно совершенные общественно опасные деяния, посягающие на нормальный порядок обращения охраняемой законом компьютерной информации, запрещенные УК РФ под угрозой наказания.

Непосредственным объектом преступлений в сфере компьютерной информации являются отношения по поводу обеспечения целостности и сохранности компьютерной информации и безопасного функционирования информационных систем.

3. Группа преступлений в сфере обращения информации и информационных систем включает в себя как преступления в сфере компьютерной информации, так и другие виды преступлений, где в качестве объекта и предмета преступления выступают информационные технологии, средства вычислительной техники и связи, реализующие информационные процессы (киберпреступления). В эту группу преступлений следует также отнести все преступления, объектом посягательства которых выступает информация. В связи с этим целесообразно назвать главу 28 УК РФ следующим образом: «Преступления в сфере обращения информации и информационных систем».

4. В целях более последовательной дифференциации ответственности за преступления, связанные с компьютерной информацией включить в УК РФ статью 146.1. в следующей редакции:

«Статья 146.1. Нарушение авторских и смежных прав на компьютерные программы

1. Присвоение авторства компьютерной программы, если это деяние причинило значительный ущерб автору или иному правообладателю, –

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо обязательными работами на срок от двухсот до двухсот сорока часов, либо исправительными работами на срок до двух лет.

2. Незаконное использование компьютерных программ, а равно приобретение, хранение, перевозка контрафактных экземпляров компьютерных программ в целях сбыта, совершенные в крупном размере, –

наказываются штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет, либо обязательными работами на срок от двухсот до двухсот сорока часов, либо лишением свободы на срок до двух лет.

3. Деяния, предусмотренные частями первой и второй настоящей статьи, если они совершены:

а) группой лиц по предварительному сговору или организованной группой;

б) в особо крупном размере;

в) лицом с использованием своего служебного положения, –

наказываются лишением свободы на срок от двух до шести лет со штрафом в размере до семисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до четырех лет либо без такового.

Примечания. 1. Значительный ущерб в настоящей статье определяется с учетом имущественного положения автора или иного правообладателя, но не может составлять менее двух тысяч пятисот рублей.

2. Деяния, предусмотренные настоящей статьей, признаются совершенными в крупном размере, если стоимость экземпляров компьютерных программ либо стоимость прав на использование объектов

авторского права и смежных прав превышает пятьдесят тысяч рублей, а в особо крупном размере – двести тысяч рублей».

5. Для усиления уголовно-правовой охраны компьютерной информации предлагается:

а) ввести в УК РФ статью 273.1:

«Статья 273.1. Использование и распространение вредоносных программ для ЭВМ

1. Использование программ для ЭВМ, которые могут привести к уничтожению, блокированию, модификации либо копированию информации, –

наказывается лишением свободы на срок до четырех лет со штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет.

2. Распространение программ для ЭВМ, которые могут привести к уничтожению, блокированию, модификации либо копированию информации, –

наказывается лишением свободы на срок до пяти лет со штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет.

3. Деяния, предусмотренные частями первой и второй настоящей статьи, повлекшие тяжкие последствия, –

наказываются лишением свободы на срок от пяти до восьми лет лишения свободы»;

б) статью 273 УК РФ изложить следующим образом:

«Статья 273. Создание вредоносных программ для ЭВМ

1. Подготовка, разработка и (или) создание программ для ЭВМ с целью использования и (или) распространения, которые могут привести к

уничтожению, блокированию, модификации либо копированию информации, –

наказываются лишением свободы на срок до трех лет.

2. Те же деяния, повлекшие по неосторожности тяжкие последствия,

– наказываются лишением свободы на срок от трех до семи лет»;

в) статью 272 УК РФ следует изложить в следующей редакции:

«1. Неправомерный доступ к охраняемой законом компьютерной информации, то есть информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, –

наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок от шести месяцев до одного года, либо лишением свободы на срок до двух лет.

2. Неправомерный доступ к компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, –

наказывается штрафом в размере до трехсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до двух лет, либо исправительными работами на срок до двух лет, либо арестом на срок до шести месяцев, либо лишением свободы на срок до пяти лет.

3. Те же деяния, совершенные группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения, а равно имеющим доступ к ЭВМ, системе ЭВМ или их сети, –

наказываются штрафом до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до трех лет, либо лишением свободы на срок до восьми лет».

г) квалифицирующий признак «нарушение работы ЭВМ, системы ЭВМ или их сети» следует исключить из статей 272-273 УК РФ, так как при совершении неправомерного доступа к охраняемой законом РФ компьютерной информации, повлекшего копирование информации и т.п., уже нарушается нормальная работа ЭВМ, системы ЭВМ или их сети.

6. Дополнить ч. 1 ст. 63 УК РФ новым отягчающим обстоятельством: в п. к) после слова «принуждения» добавить словосочетание «или с использованием компьютерной техники».

7. Статью 274 исключить из УК РФ.

8. В целях укрепления правовой основы противостояния преступлениям в сфере компьютерной информации ратифицировать Конвенцию Совета Европы о киберпреступности от 23 ноября 2001 года.

Теоретическая значимость исследования. Содержащиеся в диссертационном исследовании теоретические положения и выводы, направленные на развитие и совершенствование общей теории правового регулирования отношений в сфере компьютерной информации, могут использоваться для дальнейших исследований, связанных с проблемой уголовной ответственности за преступления в сфере компьютерной информации и преступления в сфере высоких технологий.

Практическая значимость выводов и предложений диссертационного исследования. Полученные результаты могут быть использованы в правотворческой деятельности по совершенствованию уголовно-правовых норм об ответственности за преступления в сфере компьютерной информации и связанные с ними правонарушения; при разработке

методик выявления и пресечения рассматриваемых преступлений; при квалификации преступных деяний; в учебном процессе – при изучении темы «Преступления в сфере компьютерной информации» в рамках курса «Уголовное право» и соответствующего спецкурса.

Апробация результатов исследования. Диссертация выполнена на кафедре уголовного права Казанского государственного университета, где проводилось ее рецензирование и обсуждение. Основные положения и выводы диссертационного исследования докладывались на заседаниях кафедры уголовного права, на Международной научно-практической конференции «Современное российское право: пробелы, пути совершенствования» в г. Пензе в 2007 г., опубликованы в пяти научных работах, в том числе две в рецензируемых журналах, включенных в перечень ВАК. Результаты исследования используются в учебном процессе в Ульяновском государственном университете.

Структура диссертации отвечает основной цели и предмету исследования. Работа состоит из введения, четырех глав, заключения, библиографического списка, включающего 312 наименований, и двух приложений.

Содержание работы

Во введении обосновывается актуальность темы исследования, излагаются цели и задачи исследования, оценивается уровень научной разработанности и практической значимости выбранной темы, формулируются основные положения, выносимые на защиту.

Первая глава «Понятие преступлений в сфере компьютерной информации» состоит из двух параграфов.

В первом параграфе «Правовое регулирование информационных отношений» раскрывается понятие «информация». В работе делается

акцент на то, что понятие информации как правового явления отличается от понятия информации в целом в силу ряда присущих ей свойств.

С точки зрения доступа можно выделить массовую информацию и информацию с ограниченным доступом. Информация с ограниченным доступом делится на три группы: государственная тайна, межгосударственные секреты, конфиденциальная информация. При рассмотрении данных понятий раскрывается понятие «тайны», устанавливается соотношение между свободой и тайной, тайной и конфиденциальной информацией, из которого видно, что конфиденциальная информация включает в себя различные виды тайн, такие как тайна личной жизни, коммерческая тайна, профессиональная тайна. Указанные виды тайн делятся на подвиды, регулируемые гражданским законодательством.

В диссертации приводятся различные подходы к определению понятия «ЭВМ» и делается акцент на то, что данное понятие приводится во вступившей в силу с 1 января 2008г. части IV ГК РФ.

Во втором параграфе «Понятие преступлений в сфере компьютерной информации в международном и российском уголовном праве» говорится об истоках появления понятия преступлений в сфере компьютерной информации. Впервые данное понятие появилось в международном уголовном праве. Затем развивалось в ряде международно-правовых актов. Наибольшее развитие указанный термин получил в Конвенции Совета Европы по борьбе с киберпреступностью. В Конвенции был определен состав киберпреступлений, даны рекомендации по унификации соответствующих норм в разных странах, что явилось большим шагом на пути развития законодательства в данном направлении.

В Российской Федерации понятие «преступлений в сфере компьютерной информации» появилось только в 90-х годах. В настоящее

время в отечественной науке уголовного права все еще нет четкого определения понятия преступлений в сфере компьютерной информации, высказываются различные мнения и по их классификации. В диссертации приводятся разные точки зрения по этому поводу. Диссертант делает вывод о том, что при определении понятия «преступлений в сфере компьютерной информации» следует учитывать их особенности: неоднородность объекта посягательства; возможность машинной информации выступать как в качестве объекта, так и в качестве средства совершения преступления; многообразие предметов и средств преступного посягательства; возможность компьютера выступать либо в качестве предмета, либо в качестве средства совершения преступления. Автором приводятся классификации, предложенные различными исследователями. Кроме того, диссертант предлагает собственную классификацию компьютерных преступлений по дополнительному объекту уголовно-правовой охраны, среди которых отношения, обеспечивающие охрану авторских и смежных прав. Автор считает, что компьютерные программы, являющиеся объектом авторских прав, нуждаются в особой уголовно-правовой охране, и предлагает ввести в УК РФ отдельную норму, направленную на защиту прав авторов компьютерных программ.

В юридической литературе существует спор о том, как квалифицировать деяния, совершаемые с использованием компьютеров. Так, ряд ученых предлагает включить в некоторые статьи УК квалифицирующий признак, указывающий на использование компьютеров, другие же, к которым относится и автор, предлагают квалифицировать такие деяния по совокупности с деяниями, предусмотренными главой 28 УК РФ. Диссертант также обосновывает переименование главы 28 УК РФ и предлагает назвать ее «Преступления в сфере обращения информации и информационных систем» в разделе

«Преступления против общественной безопасности и общественного порядка».

В главе второй «Юридический анализ составов преступлений в сфере компьютерной информации» дается характеристика составов преступлений, предусмотренных главой 28 УК РФ.

В первом параграфе «Неправомерный доступ к компьютерной информации» раскрываются объективные и субъективные признаки составов преступлений, предусмотренных статьей 272 УК РФ.

Придерживаясь понимания объекта преступления как охраняемых уголовным законом общественных отношений, автор указывает, что непосредственным объектом неправомерного доступа к компьютерной информации являются отношения по поводу обеспечения целостности и сохранности компьютерной информации и безопасного функционирования информационных систем. Предметом данного преступления является компьютерная информация. Объективная сторона преступления выражается в форме действия – доступа. Неправомерный доступ к компьютерной информации может быть как непосредственным, так и удаленным или смешанным. В качестве необходимых признаков объективной стороны в статье 272 указываются и общественно опасные последствия в виде уничтожения, модификации, блокирования, копирования информации, нарушения работы ЭВМ, системы ЭВМ, их сети и причинная связь между деянием и последствиями. Однако сам факт неправомерного доступа может повлечь и иные последствия (возможность ознакомиться и распорядиться информацией). Поэтому предлагается считать состав оконченным после получения доступа к компьютерной информации. Понятие общественно опасных последствий применительно к данному составу преступления носит в теории уголовного права дискуссионный характер. Одно из таких последствий – копирование

информации, под которым автор понимает воспроизведение или запись охраняемой законом компьютерной информации на носителе, отличном от исходного. Следующим последствием неправомерного доступа к компьютерной информации является ее уничтожение. При рассмотрении вопроса об уничтожении компьютерной информации автор указывает на то, что в теории отмечаются различные подходы к пониманию указанного понятия. Ряд авторов отмечает, что при уничтожении компьютерной информации зачастую сохраняется возможность восстановить ее при помощи специальных программных средств. Диссертант полагает, что при совершении преступления виновному неизвестно, имеется ли возможность восстановления уничтоженной информации или нет. Поэтому под уничтожением компьютерной информации диссертант понимает удаление ее из памяти ЭВМ или машинного носителя, когда доступ к ней законного пользователя или владельца невозможен, независимо от возможности ее восстановления. При определении такого последствия, как модификация, автор указывает на то, что важнейшим элементом данного понятия является направленность его на изменение информации. В противном случае это не модификация, а уничтожение информации. Под блокированием информации диссертант понимает создание условий, при которых невозможно или существенно затруднено использование информации при сохранности такой информации. Под нарушением работы ЭВМ, системы ЭВМ или их сети понимается временное или устойчивое создание помех для их функционирования в соответствии с назначением. Автор предлагает исключить данный признак из УК РФ, так как при совершении неправомерного доступа к компьютерной информации уже нарушается нормальная работа ЭВМ, системы ЭВМ или их сети.

Во втором параграфе «Создание, использование и распространение вредоносных программ для ЭВМ» дается характеристика объективных и

субъективных признаков состава преступления, предусмотренного статьей 273 УК РФ. Непосредственным объектом данного состава преступления являются общественные отношения по обеспечению безопасности компьютерной информации, а также безопасности функционирования программ для ЭВМ.

Объективная сторона рассматриваемого преступления характеризуется действием – созданием вредоносной программы или внесением изменений в существующие программы, использованием или распространением таких программ или машинных носителей с такими программами. Вопрос о создании вредоносной программы является дискуссионным. Ряд ученых считает, что признаками данного состава охватываются «этапы» создания программы, т.е. те моменты, в которые она находится еще в стадии оформления. Диссертант же указывает на то, что без надлежащего оформления вредоносная программа не представляет опасности. Автор полагает, что программа является созданной тогда, когда она станет пригодной для непосредственного выполнения без какого-либо предварительного преобразования.

Определение программы для ЭВМ дано в статье 1261 ГК РФ. Вредоносной же программой следует считать представленную в объективной форме совокупность данных и команд, предназначенных для ЭВМ и других компьютерных устройств в целях получения определенного результата в виде уничтожения, блокирования, модификации, либо копирования информации, нарушения работы ЭВМ, системы ЭВМ или их сети, а также других негативных последствий. Под внесением изменений в существующие программы следует понимать модификацию информации. К пониманию понятия «использование вредоносной программы» так же существуют различные подходы. Под

использованием такой программы автор понимает запуск ее в ЭВМ, системе ЭВМ или их сети, а под распространением – передачу как с помощью специальных носителей, сети, так и иным другим способом другому лицу. Автор отмечает, что, как показывает практика, распространение вредоносных программ может осуществляться наряду с другими преступлениями или для подготовки к ним.

Часть 2 статьи 273 УК РФ в качестве квалифицирующего признака указывает на причинение по неосторожности тяжких последствий. При этом «тяжкие последствия» – оценочная категория, которая подлежит оценке судом. Автор полагает, что в примечании к статье 273 или в тексте самой статьи необходимо указать примерный перечень таких последствий, как это сделано в УК Республики Беларусь. Состав считается оконченным с момента наступления указанных последствий.

В третьем параграфе «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети» даются характеристики объективных и субъективных признаков состава, предусмотренного статьей 274 УК РФ. Объект преступления – отношения, обеспечивающие безопасность в сфере эксплуатации ЭВМ, системы ЭВМ или их сети.

Объективная сторона характеризуется как действием **(**например, использование служебных аппаратных и программных средств в личных целях), так и бездействием **(**например, непроведение обязательного резервного копирования базы данных). В качестве обязательного признака статья 274, как и статья 272, предусматривает наступление общественно-опасных последствий: во-первых, нарушение специальных правил должно повлечь уничтожение, блокирование или модификацию охраняемой законом компьютерной информации, во-вторых, уничтожение, блокирование или модификация информации должны причинить существенный вред. С субъективной стороны деяние может

характеризоваться виной как в форме умысла (чаще – косвенного), так и в форме неосторожности. Иная ситуация предусмотрена частью второй статьи 274: здесь тяжкие последствия в результате нарушения специальных правил причиняются исключительно по неосторожности, в противном случае деяние следует квалифицировать по фактически наступившим последствиям. Субъект данного преступления – вменяемое лицо, достигшее 16 лет, имеющее доступ к ЭВМ, системе ЭВМ или их сети. Из всех норм о преступлениях в сфере компьютерной информации данная норма характеризуется наивысшей степенью латентности из-за сложностей установления объективной стороны, размытости самой нормы. Правильнее было бы исключить ее из УК РФ. В Конвенции Совета Европы о киберпреступности нет аналогов статьи 274, подобных норм нет и в зарубежном законодательстве. Как показала практика применения УК РФ, данное нововведение отечественного законодателя оказалось не востребованным, т.е. ни одно уголовное дело за последние годы по данной статье не возбуждалось.

Третья глава «Назначение наказания за преступления в сфере компьютерной информации» содержит два параграфа.

Первый параграф «Механизм достижения целей наказания за преступления в сфере компьютерной информации» описывает механизм достижения целей наказания, включающий в себя ряд структурных элементов. Раскрывая указанные структурные элементы механизма, автор делает вывод о необходимости включить в УК РФ норму, посвященную использованию компьютерной техники при совершении преступления: включить словосочетание «….с использованием компьютерной техники» в ст. 63 УК РФ в п. к). Диссертант предлагает учитывать это при назначении наказания, т.к. с использованием компьютерной техники, как указывалось ранее, совершается достаточно большое количество преступлений,

предусмотреть в каждом составе преступления такой квалифицирующий признак не представляется возможным, поэтому целесообразно ввести соответствующее отягчающее обстоятельство в статью 63 УК РФ.

Автором проанализирована практика назначения наказания за преступления в сфере компьютерной информации и сделан вывод о том, что суд, как правило, не усматривает в деле отягчающих обстоятельств. Это связано как с личностью самого преступника, так и с обстоятельствами преступления. Так, преступления в сфере компьютерной информации совершаются лицами, имеющими высшее или среднее специальное образование, не имеющими отрицательных характеристик по месту работы или учебы, в основном лицами молодого возраста. Большое значение при назначении наказания за преступления в сфере компьютерной информации имеет достижение цели предупреждения преступлений, в том числе и общего предупреждения. Преступление в сфере компьютерной информации не может быть совершено с особой жестокостью, садизмом, а также с рядом других отягчающих обстоятельств. В то же время немногочисленная практика свидетельствует, что чаще всего при назначении наказания за преступления в сфере компьютерной информации учитываются смягчающие обстоятельства, такие как совершение преступления впервые, молодой возраст, признание вины в содеянном, состояние здоровья (наличие тяжелых заболеваний), готовность возместить ущерб, положительная характеристика по месту жительства и учебы, отсутствие вреда от преступления и другие.

Во втором параграфе «Назначение наказания за преступления в сфере компьютерной информации по уголовному праву России» анализируются наказания, закрепленные в санкциях статей 272-274 УК РФ и практика их применения.

Автор подробно рассматривает такие виды наказания, как штраф, исправительные работы, обязательные работы, лишение права занимать определенные должности или заниматься определенной деятельностью, ограничение свободы, лишение свободы, арест. Автор указывает, что штраф назначается, как правило, в тех случаях, когда собственнику компьютерной информации причиняется большой материальный ущерб. Наказание в виде штрафа является эффективным, но оно применимо не ко всем лицам. Так, при назначении наказания за преступления в сфере компьютерной информации суд учитывает следующие обстоятельства: отсутствие самостоятельного заработка у виновного, наличие малолетних детей на иждивении или нетрудоспособных родителей. В таких ситуациях применяются другие виды наказаний. Диссертант отмечает, что наличие альтернативных видов наказаний, бесспорно, является большим плюсом. В литературе спорят о соответствии санкций норм главы 28 УК РФ характеру и степени общественной опасности деяний. Одни ученые полагают, что санкции норм данной главы слишком суровы, другие же, наоборот, предлагают ужесточить наказание за преступления в сфере компьютерной информации. Диссертант отмечает, что санкции норм, предусмотренных статьями 272-273 УК РФ, в целом соответствуют характеру и степени общественной опасности деяний, но при этом указывает, что корректировка их необходима. В том числе автор предлагает расширить перечень наказаний, назначаемых за преступления в сфере компьютерной информации. Автор выражает свое несогласие с позицией ряда исследователей о необходимости привлечения к уголовной ответственности за преступления в сфере компьютерной информации лиц, достигших 14-летнего возраста. Исходя из принципа экономии уголовной репрессии, в данном случае следует разрабатывать комплекс превентивных мер.

Четвертая глава «Преступления в сфере компьютерной информации по зарубежному законодательству» включает в себя два параграфа.

Первый параграф «Дифференциация ответственности за преступления в сфере компьютерной информации в странах СНГ и Балтии» посвящен нормам о преступлениях в сфере компьютерной информации в Азербайджане, Грузии, Кыргызстане, Казахстане, Беларуси, Узбекистане, Туркменистане. После анализа норм указанных стран автор делает вывод, что кодексы большинства республик повторяют нормы УК РФ, однако такие республики, как Беларусь, Таджикистан, опережают российское законодательство в этом направлении.

Далее автор приводит анализ уголовного законодательства Эстонии, Литвы и Молдовы и говорит о возможности заимствования нормы о незаконном использовании компьютеров, компьютерных систем или компьютерных сетей из УК Эстонии для квалификации преступлений, в которых компьютерная техника использовалась как средство совершения преступления.

Диссертант делает вывод об отсутствии унифицированного подхода к регламентации ответственности за преступления в сфере компьютерной информации в странах СНГ и Балтии и необходимости сотрудничества государств в этом направлении.

Второй параграф называется «Дифференциация ответственности за преступления в сфере компьютерной информации в романо-германской и англо-американской правовых системах». В данном параграфе приводится анализ уголовного законодательства, в частности, норм о преступлениях в сфере компьютерной информации, таких стран, как США, Канада, Франция, Германия, Англия, Италия, Испания, Австрия, Бельгия, Дания,

Финляндия, Греция, Ирландия, Люксембург, Голландия, Португалия, Австралия, Швеция, Польша.

При характеристике зарубежного законодательства прослеживается отсутствие унифицированного подхода к описанию состава неправомерного доступа к компьютерной информации. В качестве объекта этого преступления в большинстве государств признается информационная безопасность (Англия, Канада). Предметом данного преступления выступают компьютерные данные. Встречается и более широкое понимание предмета – как информации или программ, предназначенных для использования в связи с электронной обработкой данных (Дания); сети компьютерных данных и услуг (Канада).

Бесспорно, законодательство стран с романо-германской и англо-американской правовыми системами качественно отличается от отечественного законодательства и законодательства стран СНГ. Это вызвано отличием правовых систем, а также разными темпами экономического развития и, следовательно, темпами научно-технического прогресса. Некоторые нормы являются специфичными, и необходимость в их включении в отечественное законодательство назреет еще не скоро. Однако есть и нормы, заимствование которых возможно и в настоящее время. В целом уголовное законодательство вышеперечисленных стран весьма отличается друг от друга (в УК некоторых стран содержится большое количество статей о преступлениях в сфере компьютерной информации, в то время как УК других государств вообще не содержит подобных норм). Следовательно, законодательствам разных стран, в том числе и России, необходимо двигаться по пути унификации. Главную роль в этом процессе должны играть международно-правовые акты. Поэтому

Российская Федерация должна ратифицировать Конвенцию ООН по киберпреступности.

В **заключении** работы представлены выводы по исследованию, обобщены предложения по совершенствованию действующего законодательства.

Основное содержание работы отражено в следующих публикациях:

а) публикации в ведущих рецензируемых изданиях, рекомендованных ВАК РФ:

1. Зубова, М.А. Неправомерный доступ к компьютерной информации и его последствия [Текст] / М.А. Зубова // «Черные дыры» в Российском Законодательстве. Юридический журнал. – М. – 2007. – № 6. – С. 358–359.

2. Зубова, М.А. Объективные и субъективные признаки создания и распространения вредоносных программ для ЭВМ [Текст] / М.А. Зубова // Ученые записки Казанского государственного университета. Серия Гуманитарные науки. – Т. 149. – Казань, 2007. – С. 254–260.

б) публикации в иных изданиях:

3. Зубова, М.А. Понятие преступлений в сфере компьютерной информации [Текст] / М.А. Зубова // Сборник аспирантских научных работ юридического факультета КГУ. Вып. 6. – Казань, 2005. – С. 219–221.

4. Зубова, М.А. Нормы о компьютерных преступлениях в уголовном законодательстве зарубежных стран, России и СНГ [Текст] / М.А. Зубова // Сборник аспирантских научных работ юридического факультета КГУ. – Вып. 7. – Т. 1. – Казань, 2006. – С. 212–218.

5. Зубова, М.А. Преступления в сфере компьютерной информации: проблемы правоприменения и пути их решения [Текст] / М.А. Зубова // Сборник статей Международной научно-практической конференции

«Современное российское право: пробелы, пути совершенствования». – Пенза, 2007. – С. 74–76.

ЗУБОВА Марина Александровна

Компьютерная информация

как объект уголовно-правовой охраны

Автореферат

Подписано в печать .09.2008
Формат 60x84/16. Гарнитура Times New Roman.
Усл. печ. л. . Уч.-изд. л. .
Тираж 100 экз. Заказ № /

Оригинал-макет подготовлен в Издательском центре
Ульяновского государственного университета
432000, г. Ульяновск, ул. Л. Толстого, 42

Отпечатано с оригинал-макета в Издательском центре
Ульяновского государственного университета
432000, г. Ульяновск, ул. Л. Толстого, 42